CLAIMS

1. A content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the content distribution server comprising:

a key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

an encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

a content receiving unit operable to receive a content via the network;

an encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and

a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses.

2. The content distribution server according to Claim 1,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0th level through an nth level (n is 1 or a larger natural number); and

selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level, and (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th through the nth level, and

the encryption key group selection unit selects the selected node encryption key group so that said selected node encryption key group includes at least a node encryption key that is set for a terminal node and a node encryption key that is set for a node other than the terminal node.

3. The content distribution server according to Claim 2,

wherein the tree structure in the key assignment method is an N-ary tree (N is 2 or a larger natural number).

4. The content distribution server according to Claim 1, further comprising

a content key generation unit operable to newly generate at least one pair of a content encryption key and a corresponding content decryption key which is different from at least one pair of a content encryption key which is previously used for encrypting a content and a corresponding content decryption key, in the case where the content receiving unit receives a new content.

5. The content distribution server according to Claim2,

wherein the encryption key group selection unit newly selects a selected node encryption key group including a node encryption key that is set for another terminal node than a previously selected terminal node, in the case of receiving a new content via the content receiving unit.

6. The content distribution server according to Claim 1, further comprising

a key selection information storage unit operable to hold a plurality of key selection information which are used for selecting the node encryption key included in the node encryption key group,

wherein the encryption key group selection unit selects the selected node encryption key group based on the key selection information.

7. The content distribution server according to Claim 6,

wherein the key selection information storage unit further holds a plurality of key selection identifiers that identify the key selection information, the key selection identifiers and the key selection information being associated with each other,

the encryption key group selection unit selects the selected node encryption key group based on the key selection information, and

the transmission unit distributes, to the content output apparatuses, the encrypted content, the encrypted content decryption key group and the key selection identifiers associated with the key selection information.

8. The content distribution server according to Claim 6,

wherein the encrypted key group selection unit selects, on a random basis, one of the key selection information from among the plurality of key selection information held in the key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information.

9. The content distribution server according to Claim 6,

wherein the encryption key group selection unit selects, at

regular intervals, one of the key selection information from among the plurality of key selection information held in the key selection information storage unit, and selects the selected node encryption key group based on the selected key selection information.

10. The content distribution server according to Claim 1, further comprising

a storage unit operable to store the node encryption key group received via the network into the key information storage unit.

11. A key assignment method for assigning a node decryption key for obtaining a content decryption key to each of content output apparatuses connected with a content distribution server v ia a network, the content distribution server distributing a content encrypted using a content encryption key, the content output apparatus receiving the encrypted content and decrypting the encrypted content using the content decryption key, and the method having one or more tree structures, in each of which a plurality of content output apparatuses serve as nodes, and comprising:

classifying the nodes into a plurality of levels from a 0th level through an nth level (n is 1 or a larger natural number);

setting one or more pairs of node encryption keys and corresponding node decryption keys for all the nodes that make up the tree structure;

selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level and (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th through the nth level;

associating one of the terminal nodes with the content output apparatus to which the content is to be distributed, and assigning, to

the output apparatus, a set of the node decryption keys which are set for respective nodes belonging to a relevant node set which is relevant to the associated terminal node, as a node decryption key group; and

distributing the node decryption key group to the content output apparatus.

12. The key assignment method according to Claim 11,

wherein the relevant node set includes at least one terminal node, a parent node of the terminal node and a series of parent nodes of the parent node, and

in the assigning, the node decryption keys which are set for the nodes belonging to the relevant node set are assigned as the node decryption key group.

13. The key assignment method according to Claim 11,

wherein a node belonging to the ith level (i is a natural number from 1 to n) in the tree structure is connected by a line to a parent node that is one of nodes belonging to the 0th level to the i-1th level, and

in the assigning, the node decryption keys corresponding to parent nodes connected by lines are assigned as the node decryption key group.

14. The key assignment method according to Claim 11,

wherein only one node belongs to the 0th level.

15. The key assignment method according to Claim 11, further comprising

setting the node encryption keys for all the nodes as a node encryption key group corresponding to the node decryption key group assigned in the assigning.

16. The key assignment method according to Claim 11,

wherein the tree structure in the key assignment method is an N-ary tree (N is 2 or a larger natural number).

17. A content output apparatus that receives an encrypted content from a content distribution server via a network, decrypts the encrypted content using a content decryption key, and outputs the decrypted content, the apparatus comprising:

a first receiving unit operable to receive the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server;

a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method;

a node key storage unit operable to hold the node decryption key group;

a decryption key obtaining unit operable to obtain the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group; and

a first decryption unit operable to decrypt the encrypted content using the content decryption key.

18. The content output apparatus according to Claim 17, further comprising

a key selection information storage unit operable to hold a plurality of key selection information of the node decryption keys in the node decryption key group and a plurality of key selection identifiers that identify the key selection information, the key selection information and the key selection identifiers being associated with each other,

wherein the first receiving unit further receives the key

selection identifiers.

19. The content output apparatus according to Claim 18,

wherein the decryption key obtaining unit obtains the content decryption key using the plurality of key selection information, based on the node decryption key group, the encrypted content decryption key group and the key selection identifier.

20. The content output apparatus according to Claim 17, further comprising:

a third receiving unit operable to receive key update information;

an individual key storage unit operable to hold a previously given individual key; and

a second decryption unit operable to decrypt the key update information received based on the individual key, and store a decrypted node decryption key group obtained by the decryption into the node key storage unit,

wherein the decryption key obtaining unit obtains the content decryption key based on the node decryption key group and the encrypted content decryption key group, and

the first decryption unit decrypts the encrypted content using the content decryption key.

21. A key issuing center that is connected, via a network, with a content distribution server and content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses, the content distribution server distributing an encrypted content to the content output apparatuses, each of which receives the encrypted content, decrypts the received content using the content decryption key and outputs the decrypted content, the key issuing center comprising:

a node key generation unit operable to generate, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus;

a first transmission unit operable to transmit the node encryption key group to the content distribution server;

a node decryption key group selection unit operable to select at least one of the node decryption keys, and generate the node decryption key group to be distributed to each content output apparatus; and

a second transmission unit operable to distribute the node decryption key group to the content output apparatus.

22. The key issuing center according to Claim 21, further comprising

a content output apparatus correspondence information storage unit operable to hold correspondence information between the generated plurality of node decryption key groups and the plurality of content output apparatuses,

wherein the second transmission unit distributes the node decryption key groups to the content output apparatuses based on the correspondence information.

23. The key issuing center according to Claim 21,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0th level through a nth level (n is 1 or a larger natural number); and

selecting a terminal node in the tree structure, the terminal

node being (i) a node that belongs to the nth level and (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th level through the nth level, and

the node decryption key selection unit selects the selected node decryption key group so that said selected node encryption key group includes at least a node encryption key that is set for a terminal node and a node encryption key that is set for a node other than the terminal node.

24. The key issuing center according to Claim 22, further comprising:

a first encryption unit operable to encrypt the node decryption key group selected by the node decryption key selection unit based on an individual key which is previously given to each content output apparatus, and generate an encrypted node decryption key group; and

a key update information generation unit operable to generate key update information based on the encryption performed by the first encryption unit,

wherein the content output apparatus correspondence information storage unit further holds the individual key, and

the second transmission unit distributes the key update information to the content output apparatuses.

25. The key issuing center according to Claim 24,

wherein the content output apparatus correspondence information storage unit further holds correspondence information between content output apparatus identifiers assigned to the content output apparatuses and the node decryption key groups,

the key issuing center further comprises

a correspondence information update unit operable to update

the correspondence information held in the content output apparatus correspondence information storage unit based on a content output apparatus identifier, and output a node key generation request to the node key generation unit, in the case of receiving the content output apparatus identifier from outside via the network, and

the node key generation unit generates the node encryption key group and the node decryption key group based on the key assignment method, in the case of receiving the node key generation request.

26. The key issuing center according to Claim 24,

wherein the node key generation unit outputs a key update information generation request to the first encryption unit, in the case of generating the node encryption key group and the node decryption key group based on the key assignment method,

the first encryption unit encrypts the node decryption key group which is assigned to each content output apparatus using the previously given individual key, in the case of receiving the key update information generation request, and

the key update information generation unit generates the key update information.

27. A content distribution system comprising content output apparatuses and a content distribution server, each of the content output apparatuses decrypting an encrypted content using a content decryption key and outputting the decrypted content, and a content distribution server creating an encrypted content by encrypting a content, and distributing the encrypted content to each content output apparatus via a network,

wherein the content output apparatus includes:

a first receiving unit operable to receive the encrypted

content and an encrypted content decryption key group which are distributed from the content distribution server;

a second receiving unit operable to receive, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method;

a node key storage unit operable to hold the node decryption key group;

a decryption key obtaining unit operable to obtain the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group; and

a first decryption unit operable to decrypt the encrypted content using the content decryption key, and

the content distribution server includes:

a key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

an encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

a content receiving unit operable to receive a content via the network;

an encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and

a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the

content output apparatuses.

28. The content distribution system according to Claim 27, further comprising a key issuing center that is connected, via a network, with the content distribution server and the content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses,

wherein the key issuing center includes:

a node key generation unit operable to generate, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus;

a first transmission unit operable to transmit the node encryption key group to the content distribution server;

a node decryption key group selection unit operable to select at least one of the node decryption keys, and generate the node decryption key group to be distributed to each content output apparatus; and

a second transmission unit operable to distribute the node decryption key group to the content output apparatus.

29. A program to be used for a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the program comprising:

holding a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

selecting, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

generating an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

receiving a content via the network;

encrypting the content using a content encryption key which is previously given as a pair with the content decryption key; and

distributing the encrypted content and the encrypted content decryption key group to the content output apparatuses.

30. A program to be used for a content output apparatus that receives an encrypted content from a content distribution server via a network, decrypts the encrypted content using a content decryption key, and outputs the decrypted content, the program comprising:

receiving the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server;

receiving, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method;

holding the node decryption key group;

obtaining the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group; and

decrypting the encrypted content using the content decryption key.

31. A program to be used for a key issuing center that is

connected, via a network, with a content distribution server and content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output apparatuses, the content distribution server distributing an encrypted content to the content output apparatuses, each of which receives the encrypted content, decrypts the received content using the content decryption key and outputs the decrypted content, the program comprising:

generating, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus;

transmitting the node encryption key group to the content distribution server;

selecting at least one of the node decryption keys, and generating the node decryption key group to be distributed to each content output apparatus; and

distributing the node decryption key group to the content output apparatus.

32. A program to be used for a key assignment method for assigning a node decryption key for obtaining a content decryption key to each of content output apparatuses connected with a content distribution server via a network, the content distribution server distributing a content encrypted using a content encryption key, the content output apparatus receiving the encrypted content and decrypting the encrypted content using the content decryption key, the method having one or more tree structures, in each of which a plurality of content output apparatuses serve as nodes, and the program comprising:

classifying the nodes into a plurality of levels from a 0th level through an nth level (n is 1 or a larger natural number);

setting one or more pairs of node encryption keys and corresponding node decryption keys for all the nodes that make up the tree structure;

selecting a terminal node in the tree structure, the terminal node being (i) a node that belongs to the nth level and (ii) a node that belongs to the jth level (j is a natural number from 1 to n-1) and is not connected by lines with any nodes belonging to the j+1th through the nth level;

associating one of the terminal nodes with the content output apparatus to which the content is to be distributed, and assigning, to the output apparatus, a set of the node decryption keys which are set for respective nodes belonging to a relevant node set which is relevant to the associated terminal node, as a node decryption key group; and

distributing the node decryption key group to the content output apparatus.

33. A computer readable recording medium on which a program according to any one of Claim 29 to Claim 32 is recorded.

34. A content distribution method to be used for a content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the method comprising:

holding a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

selecting, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

generating an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using said at least one node encryption key in the selected node encryption key group;

receiving a content via the network;

encrypting the content using a content encryption key which is previously given as a pair with the content decryption key; and

distributing the encrypted content and the encrypted content decryption key group to the content output apparatuses.

35. A content distribution method to be used for a content output apparatus that receives an encrypted content from a content distribution server via a network, decrypts the encrypted content using a content decryption key, and outputs the decrypted content, the method comprising:

receiving the encrypted content and an encrypted content decryption key group which are distributed from the content distribution server;

receiving, via the network, a node decryption key group which is previously assigned by a predetermined key assignment method;

holding the node decryption key group;

obtaining the content decryption key based on at least one node decryption key group and at least one encrypted content decryption key group; and

decrypting the encrypted content using the content decryption key.

36. A content distribution method to be used for a key issuing center that is connected, via a network, with a content distribution server and content output apparatuses, and issues a key for obtaining a content decryption key to each of the content output

apparatuses, the content distribution server distributing an encrypted content to the content output apparatuses, each of which receives the encrypted content, decrypts the received content using the content decryption key and outputs the decrypted content, the method comprising:

generating, based on a predetermined key assignment method, a node encryption key group that is a set of node encryption keys and a node decryption key group that is a set of node decryption keys, each of the node encryption keys and node decryption keys being assigned to each content output apparatus;

transmitting the node encryption key group to the content distribution server;

selecting at least one of the node decryption keys, and generating the node decryption key group to be distributed to each content output apparatus; and

distributing the node decryption key group to the content output apparatus.